UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/561,896	12/21/2005	Gerardus T.M. Hubert	GB030098US1	1091

65913 7590 05/21/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
NGUYEN, TRONG H	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
05/21/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/561,896	HUBERT, GERARDUS T.M.	
	Examiner	Art Unit	
	TRONG NGUYEN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 18-30* is/are pending in the application.

4a) Of the above claim(s) *16,17 and 31-33* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 18-30* is/are rejected.

7)☒ Claim(s) *1-15,18 and 23-30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on **02/17/2009**. In response to the office action mailed on **11/14/2008**, **claims 1-15 and 18-30** have been amended and **claims 16-17 and 31-33** have been canceled. Pending claims include **claims 1-15** and **18-30**.

The objection to the abstract has been withdrawn due to Applicant's amendment.

The objection to title of the specification has been withdrawn due Applicant's amendment.

The objection to the specification has been withdrawn due to Applicant's persuasive arguments.

The objection to **claims 1, 5, 13, 18, 22 and 28** has been withdrawn due to Applicant's amendments.

The rejection of **claims 1, 6-8, 10, 18, 21, 23-25, 27 and 30** under 35 USC 112, second paragraph has been withdrawn due to Applicant's amendment.

The rejection of **claims 9-10 and 26-27** under 35 USC 112, second paragraph for insufficient antecedent basis for "k-2", has been withdrawn due to Applicant's persuasive argument.

The rejection of **claims 1-15 and 18-30** under 35 USC 101 has been withdrawn due to Applicant's amendment.

Examiner Notes

2. Examiner respectfully requests that Applicant considers including equations describing variables (i.e. n_0, r_0, r_1, r_2, and B) and their relationships into the claims in order to clarify and help place the application in better condition for allowance.

Response to Arguments

3. Applicant's arguments with respect to **claims 1 and 18** have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. **Claims 1-15, 18 and 23-30** objected to because of the following informalities:

It is unclear whether "a fourth variable Br_2" on line 11 of **claim 1** refers to a product of B multiplying by r_2 or a result of B concatenates with r_2.

"A method" on line 1 of **claims 2-13** should be "The method".

"the combined multiplication operations and reduction operation" on line 2 of **claim 4** lacks antecedent basis.

"when" on line 2 of **claims 6 and 7** should be omitted or amended in such as way as to avoid the current language ambiguities as to whether the limitations that follow it are actually further limiting/necessary/occurring.

"the next multiplication" on line 3 of **claim 8** lacks antecedent basis.

"the number of leading '1'" on line 2 of **claim 9** lacks antecedent basis. Moreover, it is unclear whether "the number" after "if" on line 2 of **claim 9** refers to "a number" on line 5 of **claim 1** or "number of leading '1'" on line 2 of **claim 9**.

"when" on line 3 of **claim 10** should be omitted or amended in such as a way to avoid the current language ambiguities as to whether the limitations that follow it are actually further limiting/necessary/occurring. Furthermore, "the number of leading '1'" on line 3 of **claim 10** lacks antecedent basis.

"when" on line 4 of **claims 14 and 15** should be omitted or amended in such as a way to avoid the current language ambiguities as to whether the limitations that follow it are actually further limiting/necessary/occurring.

"...modulus performs..." on line 11 of **claim 18** should be "...modulus and performs...". In addition, it is unclear whether "a fourth variable Br_2" on line 16 of **claim 18** refers to the product of B multiplying by r_2 or the result of B concatenates with r_2.

"when" on line 3 of **claims 23 and 24** should be omitted or amended in such as a way to avoid the current language ambiguities as to whether the limitations that follow it are actually further limiting/necessary/occurring.

"the next multiplication" on line 4 of **claim 25** lacks antecedent basis.

"Apparatus" on line 1 of **claim 26** should be "The apparatus". In addition, "the number of leading '1'" on line 2 of **claim 26** lacks antecedent basis. Moreover, it is unclear whether "the number" after "if" on line 2 of **claim 26** refers to "a number" on line 10 of **claim 18** or "number of leading '1'" on line 2 of **claim 26**.

"when" on line 3 of **claim 27** should be omitted or amended in such as a way to avoid the current language ambiguities as to whether the limitations that follow it are actually further limiting/necessary/occurring. Furthermore, "the number of leading '1'" on line 3 of **claim 27** lacks antecedent basis.

"with means for 192-bit ECC and a word size of 64-bit" on line 3 of **claim 28** is unclear.

"with means for 128-bit ECC and a word size of 64-bit" on line 3 of **claim 29** is unclear.

"with means, for 256-bit ECC and word size of 64-bit" on line 3 of **claim 30** is unclear.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-5, 14-15 and 18-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollmann et al US 6,366,673 (hereinafter "Hollmann") in view of Koc et al. US 2002/0059353 A1 (hereinafter "Koc").

Regarding **claim 1**, Hollmann discloses **a method of performing a reduction operation in a cryptographic calculation in a digital computer,** [modified Quisquater method (Col. 5, line 16)] **the method comprising**:

selecting a modulus having a first section with a plurality of "1" Most Significant Word states and a second section which further comprises: a plurality of "1" or "0" states [first p most significant bits of N are all equal to 1 (first section) and (n-p) bits may be "1" or "0" states (second section) (Col. 4, lines 3-4)] **whereby a**

number formed of the two sections is a modulus; [N is a modulus (Col. 4, lines 3-4 and Col. 5, lines 17-18)] **and**

operating a reduction operation on the modulus [calculating z in inner loop (Col. 9, line 18 and Col. 9, lines 65-66)]

but Hollmann does not specifically disclose

multiplying a first variable $n_{0'}$ by a second variable r_3 to produce a first result; although Koc does suggest similar step being performed such as the operation (i.e. multiplying) and variables (i.e. $n_{0'}$ and r_3) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variables as recited below;

adding the first result to a third variable r_1 and a fourth variable Br_2 to produce a first sum; although Koc does suggest similar step being performed such as the operation (i.e. adding) and variables (i.e. r_1 and Br_2) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variables as recited below;

dividing the first sum into an upper half and a lower half; although Koc does suggest similar step being performed such as the operation (i.e. dividing) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step as recited below;

multiplying the upper half by the first variable $n_{0'}$ to produce a second result; although Koc does suggest similar step being performed such as the operation

(i.e. multiplying) and variable (i.e. $n_{0'}$) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variable as recited below;

adding the second result to the lower half and a fifth variable r_0 to produce a second sum, thereby permitting use of the second sum as the modulus. although Koc does suggest similar step being performed such as the operation (i.e. adding) and variable (i.e. r_0) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variable as recited below;

However, Koc does discloses

i. multiplying a first variable M by a second variable P_1 to produce a first result (Col. 6, Table 6, step 10-11 when i=0)

ii. adding the first result to a third variable T_1 and a fourth variable c (Col. 6, Table 6, step 10-11 when i=0)

iii. dividing a sum AB + p(Abp' mod R) into an upper half and a lower half (Col. 5, eq. 16)

Furthermore, **multiplying the upper half by the first variable $n_{0'}$ to produce a second result**; and **adding the second result to the lower half and a fifth variable r_0 to produce a second sum** are reiteration of the same operations performed in i and ii above. Koc also discloses reiteration of the same operations on Col. 6, Table 6, steps 10-11 when i=1.

Whereas, Hollmann does disclose

i. multiplying a first variable M (since z<-Mult(u,v; M) by a second variable F to produce a first result (Col. 9, line 18)

ii. adding the result to a third variable u multiplied by v_0 and a fourth variable u multiplied by $v_{\text{upper limit of i}}$ to produce a first sum h (Col. 9, line 18)

iii. dividing the first sum h into an upper half h/a^n and a lower half h (Col. 9, line 29)

iv. multiplying the upper half h/a^n by the first variable M to produce a second result (Col. 9, line 29)

v. adding the second result to the lower half h (Col. 9, line 29) and a fifth variable z (Col. 9, line 20) to produce a second sum, thereby permitting use of the second sum as the modulus.

Koc and Hollmann are analogous art because they are in the same field of endeavor of modular reduction.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's invention by including **multiplying a first variable $n_{0'}$ by a second variable r_3 to produce a first result**; **adding the first result to a third variable r_1 and a fourth variable Br_2 to produce a first sum**; **dividing the first sum into an upper half and a lower half**; **multiplying the upper half by the first variable $n_{0'}$ to produce a second result**; and **adding the second result to the lower half and a fifth variable r_0 to produce a second sum, thereby permitting use of the second sum as the modulus** since steps and procedures such as multiplying, adding and dividing are common in a reduction operation dealing with modular arithmetic as described by Koc (Col.1, Pars. 0003 and 0057, line 1).

Regarding claim **2**, Hollmann in view of Koc discloses "**A method according to claim 1 further comprising: effecting a plurality of multiplication operations**" as [calculating h in inner loop (Hollmann, Col. 9, line 17 and Col. 9, lines 65-66)].

Regarding claim **3**, Hollmann in view of Koc discloses "**A method according to claim 2 further comprising: effecting a plurality of multiplication operations followed by effecting a reduction operation**" as [h calculations are followed by z calculations (Hollmann, Col. 9, line 17-18 and Col. 9, lines 65-66)].

Regarding claim **4**, Hollmann in view of Koc discloses "**A method according to claim 3 further comprising: repeating the combined multiplication operations and reduction operation**" as [h and z calculations are repeated (Hollmann, Col. 9, line 16-18 and Col. 9, lines 65-66)].

Regarding claim **5**, Hollmann in view of Koc discloses "**A method according to claim 1 further comprising: using a multiple of the modulus**" as [all intermediate computations are done modulo N instead of modulo M where N is a multiplicity of M (Hollmann, Col. 5, lines 21-22)].

Regarding claim **14**, Hollmann in view of Koc discloses "**A computer program product directly loadable into the internal memory of a digital computer, comprising: software code portions for performing the method of claim 1 when said product is run on a computer**" as [As indicated in Hollmann's figures 1 and 2, the method of claim **1** is implemented in a computer system which inherently includes a software that performs the intended method. Also, see rejection of claim **1** for rejection of the method].

Regarding claim **15**, Hollmann in view of Koc discloses "**A computer program directly loadable into the internal memory of a digital computer, comprising: software code portions for performing the method of claim 1 when said program is run on a computer**" as [As indicated in Hollmann's figures 1 and 2, the method of claim **1** is implemented in a computer system which inherently includes a software that performs the intended method. Also, see rejection of claim **1** for rejection of the method].

Regarding claim **18**, Hollmann discloses "**An apparatus that performs a reduction operation in a cryptographic calculation on a digital computer**," as [device for performing a reduction operation (Fig. 1, Col. 7, line 57)] "**the apparatus comprising:**

a plurality of input registers that store a plurality of input operands; [input registers 26 and 30 (Fig. 1)]

a plurality of output registers that store a plurality of outputs; and [result register 28, selecting register 32 and memory 20 (Fig. 1)]

a multiplier that produces said outputs using a function that operates on variables from both said input registers and said output registers; [Fig. 1 and Col. 8, lines 2-7)]

wherein said multiplier selects a modulus having a first section with a plurality of "1" states and a second section having a plurality of "1" or "0" states" as [first p most significant bits of **N** are all equal to 1 (first section) and (n-p) bits may be "1" or "0" states (second section) (Col. 4, lines 3-4)] "**whereby a number formed of the**

two sections is a modulus" as [N is a multiple of modulus M (Col. 4, lines 3-4 and Col. 5, lines 17-18)] "**performs a reduction operation on the modulus**" as [calculating z in inner loop (Col. 9, line 18 and Col. 9, lines 65-66)]

but Hollmann does not specifically disclose

multiplying a first variable $n_{0'}$ by a second variable r_3 to produce a first result; although Koc does suggest similar step being performed such as the operation (i.e. multiplying) and variables (i.e. $n_{0'}$ and r_3) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variables as recited below;

adding the first result to a third variable r_1 and a fourth variable Br_2 to produce a first sum; although Koc does suggest similar step being performed such as the operation (i.e. adding) and variables (i.e. r_1 and Br_2) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variables as recited below;

dividing the first sum into an upper half and a lower half; although Koc does suggest similar step being performed such as the operation (i.e. dividing) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step as recited below;

multiplying the upper half by the first variable $n_{0'}$ to produce a second result; although Koc does suggest similar step being performed such as the operation (i.e. multiplying) and variable (i.e. $n_{0'}$) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variable as recited below;

adding the second result to the lower half and a fifth variable r_0 to produce a second sum, thereby permitting use of the second sum as the modulus. although Koc does suggest similar step being performed such as the operation (i.e. adding) and variable (i.e. r_0) as found in the applicant's independent claim 1 and Hollmann does suggest example of this similar step and variable as recited below;

However, Koc does discloses

i. multiplying a first variable M by a second variable P_1 to produce a first result (Col. 6, Table 6, step 10-11 when i=0)

ii. adding the first result to a third variable T_1 and a fourth variable c (Col. 6, Table 6, step 10-11 when i=0)

iii. dividing a sum AB + p(Abp' mod R) into an upper half and a lower half (Col. 5, eq. 16)

Furthermore, **multiplying the upper half by the first variable n_0, to produce a second result**; and **adding the second result to the lower half and a fifth variable r_0 to produce a second sum** are reiteration of the same operations performed in i and ii above. Koc also discloses reiteration of the same operations on Col. 6, Table 6, steps 10-11 when i=1.

Whereas, Hollmann does disclose

i. multiplying a first variable M (since z<-Mult(u,v; M) by a second variable F to produce a first result (Col. 9, line 18)

ii. adding the result to a third variable u multiplied by v_0 and a fourth variable u multiplied by $v_{\text{upper limit of i}}$ to produce a first sum h (Col. 9, line 18)

iii. dividing the first sum h into an upper half h/a^n and a lower half h (Col. 9, line 29)

iv. multiplying the upper half h/a^n by the first variable M to produce a second result (Col. 9, line 29)

v. adding the second result to the lower half h (Col. 9, line 29) and a fifth variable z (Col. 9, line 20) to produce a second sum, thereby permitting use of the second sum as the modulus.

Koc and Hollmann are analogous art because they are in the same field of endeavor of modular reduction.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's invention by including **multiplying a first variable $n_{0'}$ by a second variable r_3 to produce a first result**; **adding the first result to a third variable r_1 and a fourth variable Br_2 to produce a first sum**; **dividing the first sum into an upper half and a lower half**; **multiplying the upper half by the first variable $n_{0'}$ to produce a second result;** and **adding the second result to the lower half and a fifth variable r_0 to produce a second sum, thereby permitting use of the second sum as the modulus** since steps and procedures such as multiplying, adding and dividing are common in a reduction operation dealing with modular arithmetic as described by Koc (Col.1, Pars. 0003 and 0057, line 1).

Regarding claim **19**, Hollmann in view of Koc discloses "**The apparatus of claim 18, further comprising: means to effect a plurality of multiplication operations**" as [calculating h in inner loop (Hollmann, Col. 9, line 17 and Col. 9, lines 65-66)].

Regarding claim **20**, Hollmann in view of Koc discloses "**The apparatus of claim 19, further comprising means: to effect a plurality of multiplication operations followed by a reduction operation**" as [h calculations are followed by z calculations (Hollmann, Col. 9, line 17-18 and Col. 9, lines 65-66)].

Regarding claim **21**, Hollmann in view of Koc discloses "**The apparatus of claim 20, further comprising: means to repeat the plurality of multiplication operations and the reduction operation**" as [h and z calculations are repeated (Hollmann, Col. 9, line 16-18 and Col. 9, lines 65-66)].

Regarding claim **22**, Hollmann in view of Koc discloses "**The apparatus of claim 18, further comprising means to use a multiple of the modulus**" as [all intermediate computations are done modulo N instead of modulo M where N is a multiplicity of M (Hollmann, Col. 5, lines 21-22)].

7. Claims **6-7** and **23-24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollmann in view of Koc and further in view of Blaker US 2002/0010730 (hereinafter "Blaker").

Regarding claim **6**, Hollmann in view of Koc discloses "**A method according to claim 1**" but does not specifically disclose "**wherein, when a last multiplication gives an overflow, the overflow is added to a part of a selected number.**"

However, Blaker discloses adding an overflow bit to an intermediate result of a multiplication operation (Col. 4, Par. 0036, lines 5-6).

Blaker, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology and computer arithmetic.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method in view of Koc by applying the concept of adding the overflow bit to an intermediate result as described by Blaker since it would provide for the purpose of reducing latency in a multiplication process (Blaker, Col. 4, Par. 0036, line 9).

Regarding claim **7**, Hollmann in view of Koc and further in view of Blaker disclose "**A method according to claim 6, wherein, when the overflow addition step produces an overflow, then the first variable n_0' is added to the overflow**" as [According to the multiplication criteria shown to be obvious in rejection of claim **1**, n_0' or its multiplicity is to be added to a selected number regardless of whether there exists an overflow or not. Claim **6**, which is dependent on claim **1,** discusses the case when there is an overflow and the overflow is added to the selected number. Therefore, as indicated in the rejections of claims **6** and **1** above, it would be obvious to add n_0' (with multiplicity of 1) and the overflow to the selected number].

Regarding claim **23**, Hollmann in view of Koc discloses "**The apparatus of claim 18**" but does not specifically disclose "**further comprising: means, when a last multiplication gives an overflow, to add the overflow to a part of a selected number**."

However, Blaker discloses adding an overflow bit to an intermediate result of a multiplication operation (Col. 4, Par. 0036, lines 5-6).

Blaker, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology and computer arithmetic.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device in view of Koc by applying the concept of adding the overflow bit to an intermediate result as described by Blaker since it would provide for the purpose of reducing latency in a multiplication process (Blaker, Col. 4, Par. 0036, line 9).

Regarding claim **24**, Hollmann in view of Koc and further in view of Blaker disclose "**The apparatus of claim 23, further comprising: means, when the overflow addition step produces an overflow, to add the first variable n_0' to the overflow**" as [According to the multiplication criteria shown to be obvious in rejection of claim **18**, n_0' or its multiplicity is to be added to a selected number regardless of whether there exists an overflow or not. Claim **23**, which is dependent on claim **18,** discusses the case when there is an overflow and the overflow is added to the selected number. Therefore, as indicated in the rejections of claims **23** and **18** above, it would be obvious to add n_0' (with multiplicity of 1) and the overflow to the selected number].

8. Claims **8-10 and 25-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollmann in view of Koc and further in view of McGregor US 6,240,436 (hereinafter "McGregor").

Regarding claim **8**, Hollmann in view of Koc discloses "**A method according to claim 1**," but does not specifically disclose "**wherein a carry c between two adjacent multiplications is effected as an addend in the next multiplication**."

However, McGregor discloses a Montgomery multiplication wherein a carry between two adjacent multiplications is added to the product of the next multiplication (Col. 8, lines 48-54).

Hollmann, Koc and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method in view of Koc by applying the concept of using the carry between two adjacent multiplications as the addend in the next multiplication as described by McGregor since it would provide for the purpose of high-speed modular reductions given fixed processor operand capacities (McGregor, Col. 2, lines 40-41 and 48).

Regarding claim **9**, Hollmann in view of Koc discloses "**A method according to claim 1**" but does not specifically disclose "**further comprising: monitoring the number of leading "1"s to determine if the number is less than (k-2)**."

However, McGregor discloses a technique for monitoring the number of leading "1"s by shifting a window of a chosen size (Col. 6, lines 25-29).

Hollmann, Koc and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method in view of Koc by using a window of a chosen size to monitor the number of leading "1"s and determine if the number is less than or greater than any certain positive number as described by McGregor since it would provide for the purpose of reducing the number of multiplications necessary to perform an operation (McGregor, Col. 6, lines 3-4).

Regarding claim **10**, Hollmann in view of Koc and further in view of McGregor discloses "**A method according to claim 9, further comprising: initiating a next calculation when the number of leading "1"s is less than (k-2)**" as [McGregor discloses after detecting a leading "1", a multiplication operation is initiated (Col. 6, lines 44-45)]

Regarding claim **25**, Hollmann in view of Koc discloses "**The apparatus of claim 18**" but does not specifically disclose "**further comprising: means to effect a carry c between two adjacent multiplications as an addend in the next multiplication**."

However, McGregor discloses a Montgomery multiplication wherein a carry between two adjacent multiplications is added to the product of the next multiplication (Col. 8, lines 48-54).

Hollmann, Koc and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device in view of Koc by applying the concept of using the carry between two adjacent multiplications as the addend in the next

multiplication as described by McGregor since it would provide for the purpose of high-speed modular reductions given fixed processor operand capacities (McGregor, Col. 2, lines 40-41 and 48).

Regarding claim **26**, Hollmann in view of Koc discloses "**Apparatus according to claim 18**" but does not specifically disclose "**further comprising: means to monitor the number of leading "1"s to determine if the number is less than (k-2)**."

However, McGregor discloses a technique for monitoring the number of leading "1"s by shifting a window of a chosen size (Col. 6, lines 25-29).

Hollmann, Koc and McGregor are analogous art because they are in the same field of endeavor of cryptology and modular reduction.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device in view of Koc by using a window of a chosen size to monitor the number of leading "1"s and determine the if the number is less than or greater than a certain positive number as described by McGregor since it would provide for the purpose of reducing the number of multiplications necessary to perform an operation (McGregor, Col. 6, lines 3-4).

Regarding claim **27**, Hollmann in view of Koc and further in view of McGregor discloses "**The apparatus of claim 26, further comprising: means to initiate a next calculation when the number of leading "1"s is less than (k-2)**" as [McGregor discloses after detecting a leading "1", a multiplication operation is initiated (Col. 6, lines 44-45)]

9. Claims **11-13 and 28-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollmann in view of Koc and further in view of Lenstra et al., Selecting Cryptographic Key Sizes, Journal of Cryptology, 14 August 2001 (hereinafter "Lenstra").

Regarding claim **11**, Hollmann in view of Koc discloses "**A method according to claim 1**" but does not specifically disclose "**the method further comprising: operating 192-bit ECC and a word size of 64-bit, the modulus comprises a first section of 138 bits and a second section of 54 bits.**"

However, Lenstra discloses key size of 192 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 6, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 138 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 192-bit ECC, 64-bit word size, modulus with a first section of 138 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method in view of Koc by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **12**, Hollmann in view of Koc discloses "**A method according to claim 1**" but does not specifically disclose "**the method further comprising: operating 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.**"

However, Lenstra disclose key size of 128 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 74 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 128-bit ECC, 64-bit word size, modulus with a first section of 74 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method in view of Koc by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **13**, Hollmann in view of Koc discloses "**A method according to claim 1**" but does not specifically disclose "**the method further comprising: operating 256-bit ECC and a word size of 64-bit, the modulus comprises a first section of 202 bits and a second section of 54 bits.**"

However, Lenstra disclose key size of 256 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 202 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 256-bit ECC, 54-bit word size, modulus with a first section of 202 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's modified Quisquater method in view of Koc by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **28**, Hollmann in view of Koc discloses "**The apparatus of claim 18**" but does not specifically disclose "**further comprising: with means for 192-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits**."

However, Lenstra disclose key size of 192 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 74 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation.

Thus, barring any unexpected result from particular selection of 192-bit ECC, 64-bit word size, modulus with a first section of 74 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device in view of Koc by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **29**, Hollmann in view of Koc discloses "**The apparatus of claim 18**" but does not specifically disclose "**further comprising: with means for 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.**"

However, Lenstra disclose key size of 128 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 74 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 128-bit ECC, 64-bit word size, modulus with a first section of 74 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device in view of Koc by selecting sections of a modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Regarding claim **30**, Hollmann in view of Koc discloses "**The apparatus of claim 18**" but does not specifically disclose "**further comprising: with means, for 256-bit ECC and word size of 64-bit, the modulus comprises first section of 202 bits and second section of 54 bits.**"

However, Lenstra disclose key size of 256 bits and word size of 64 bits are well known in cryptosystems and the key size and block size can vary (page 260, sec 2.2.1, lines 5-13). Furthermore, a modulus with a first section of 202 bits and a second section of 54 bits is an example of a combination of bits that is selected for an ECC operation. Thus, barring any unexpected result from particular selection of 256-bit ECC, 64-bit word size, modulus with a first section of 202 bits and a second section of 54 bits, it would have been obvious to select those particular numbers.

Lenstra, Koc and Hollmann are analogous art because they are in the same field of endeavor of cryptology.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Hollmann's device in view of Koc by selecting sections of a

modulus to be of certain sizes and the key size and the word size as described by Lenstra since they are parameters that were used in the best-known cryptosystems (Lenstra, page 260, section 2.2.1, lines 5-6).

Conclusion

10. Applicant's amendments necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/T. N/
Examiner